

UNITED STATES DISTRICT COURT

FILED

MAY 17 2024

for the

Northern District of Oklahoma

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
 iPhone 15, Model A2849, Currently Stored at the FBI)
 Tulsa Resident Office, located at 8023 E 63rd Pl,)
 Tulsa, OK)

Case No.

24mj-367-CDL**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

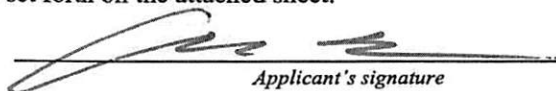
18 U.S.C. §§ 1151, 1152, and 2242(3)
 18 U.S.C. § 2261A(2)
 18 U.S.C. § 1512(b)(1)

Sexual Abuse without Consent in Indian Country
 Cyberstalking
 Witness Tampering

The application is based on these facts:

See Affidavit of SA Audra Rees, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Audra Rees, Special Agent FBI

Printed name and title

Subscribed and sworn to by phone.

Date: May 17, 2024

City and state: Tulsa, Oklahoma



Judge's signature

Christine D. Little, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
*iPhone 15, Model A2849, Currently
Stored at the FBI Tulsa Resident Agency,
located at 8023 E 63rd Pl, Tulsa, OK***

Case No. _____

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Audra Rees, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I have been employed as a Special Agent with the Federal Bureau of Investigation since January of 2020. I am currently assigned to work Indian Country Investigations for the Oklahoma City Division, Tulsa RA. As part of my duties as a Special Agent, I investigate criminal

violations relating to crime in Indian Country, to include Sexual Abuse without Consent in Indian Country, Cyberstalking, and Witness Tampering.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2261A (Cyberstalking), and 18 U.S.C. § 1512 (Witness Tampering), and 18 U.S.C. §§ 1151, 1152 and 2242(3) (Sexual Abuse without Consent in Indian Country) will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

Identification of the Device to be Examined

5. The property to be searched is an Apple iPhone 15, Model A2849, hereinafter the "Device." The Device is currently located at the FBI Tulsa Resident Agency, located at 8023 E 63rd Pl, Tulsa, OK.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

7. On March 18, 2024, B.R. reported that her ex-boyfriend, Michael Vincent MARTIN, had raped her the night before, March 17, 2024. B.R. said that MARTIN showed up at her house the night before, located at 2020 South 14th Street, Broken Arrow, Oklahoma, which is within the Cherokee Nation in the Northern District of Oklahoma. MARTIN was drunk when he arrived and continued to drink at her house. B.R. decided to go to bed because MARTIN was being “hateful” towards her. Based on previous altercations with him, B.R. turned on her phone to record any interactions with MARTIN. Shortly after she went to the bedroom, MARTIN came into her room, took off his pants, and got into bed with her. MARTIN can be heard on the recording saying, “Should I drive home on Saint Patrick’s Day, or should I have sex with the sleeping girl?” B.R. says “no.” MARTIN began touching her and performing oral sex on her and says, “You shush, and I’ll do this.” He then says, “I know you want it, you can’t say no.” B.R. says, “no” again. B.R. tried to push MARTIN away with her feet but was afraid to resist too much because he has gotten violent with her in the past. MARTIN then began having sex with B.R. She told MARTIN to stop two or three more times and was crying. B.R. finally yells at MARTIN to “fucking stop” while she’s crying. MARTIN says, “if you want me to stop, I will stop.” Martin continued to have sex with B.R. for approximately 10 more

seconds before stopping. As he is leaving, MARTIN says, "are you going to accuse me of something now?" B.R. tells MARTIN to just leave. MARTIN says he is sorry and leaves the house.

8. B.R. underwent a Sexual Assault Nurse Examination (SANE) on March 18, 2024.

9. On or about April 22, 2024, investigators accessed a link to a Google Drive provided by B.R. The Google Drive contained several different pieces of information. One of those was a folder titled "Emails after 03-17-2024".

10. This folder contained 95 screenshots of emails between MARTIN and B.R.

11. On March 18, 2024, MARTIN sent B.R. an email. In the email, he wrote: "What is going on? Why are you threatening me? The wedding you're in. What's going on?" B.R. replied with "You are not being threatened. Do not contact me again." MARTIN continued sending emails, and, near the bottom of the email said, "see you tomorrow night."

12. On March 19, 2024, MARTIN emailed B.R. many times. MARTIN told B.R. that he had "pushed the red button" and that he had to "strike back." MARTIN told B.R. he filed a protective order against her and a DHS case. Later, MARTIN told B.R., "I almost regret what I did today. Nah. You're evil. You'll see a field petition tomorrow and I hope you're back in time to be served. It'll probably happen Thursday actually so never mind." B.R. responded, "you filed a PO on me for what? And then why are you contacting me?" MARTIN told B.R. it was way worse than

just a protective order, and that “the box has been opened” and she “asked for it.” MARTIN then said, “I’ll take it back I’m sorry ☹ I’m sorry. I’ll take it back. I’ll call DHS I’ll try.” B.R. told MARTIN she would appreciate it, and then MARTIN calls her a “dumbass” and tells her that the protective order is just a precursor, and that he’s reporting her for child abuse, child neglect and various other charges.

13. On March 19, 2024, MARTIN emailed B.R. and told her there is no “red button babe. I don’t know what threats you thought I was making about getting you in trouble for something that doesn’t exist something I can’t name.” MARTIN continues on before saying, “Before you go calling the police, I will not contact you again for the record. If you think, I don’t accept responsibility for things on my own, try having a conversation about it.”

14. On March 20, 2024, MARTIN emailed B.R. and told her that he was just trying to spook her, nothing he said is true, he didn’t talk to anyone and hasn’t done anything. MARTIN told her that he’s sorry he made those “fake threats of getting you in trouble. They’ve all been fake.”

15. Later on, March 20, 2024, MARTIN told B.R. “you ever claimed that I did anything that’s a crime around you again believe me I will push the red button....”

16. MARTIN emailed B.R. on or about March 24, 2024, “Nah man. You’re fucked up. You think my messaging you 100 times means I want you back.”

17. MARTIN emailed B.R. on or about March 24, 2024, "you'll pay for your false accusations you made in that post," and "god i dont want to do it," and "try me bitch." MARTIN tells B.R. to stop "claiming victim hood."

18. In total, MARTIN emailed B.R. more than 300 times over the course of a week. These emails caused and were reasonably expected to cause substantial emotional distress to B.R.

19. On March 24, 2024, MARTIN called B.R. and she recorded the phone call. On the call, MARTIN is intoxicated and alternates between sobbing and yelling, and many parts are unintelligible. MARTIN says he's not an evil person, and maybe the alcohol made him a different person. He tells B.R. repeatedly that he loves her. MARTIN tells her that he doesn't know why she's angry. MARTIN said that B.R. lured him in so she could "claim rape" when it was "gray area" and she's not going to give him a chance to explain. B.R. told MARTIN that she told him "no" several times. MARTIN said that if that's how she felt then he's really sorry. MARTIN said he just didn't want to be accused of rape if she's recording it. B.R. asked MARTIN if he felt guilty for what he did. MARTIN says "yes, yes, yes." While sobbing, MARTIN says something about "punish fucking" B.R. because she slept with someone else. MARTIN then starts yelling at B.R. and told her that she made it a "gray area" on purpose so she could claim rape. MARTIN continues yelling and B.R. hung up the phone.

20. The FBI began investigating this case on April 5, 2024. On May 1, 2024, I made an appointment to meet with B.R. on May 6, 2024.

21. On May 4, 2024, B.R. and MARTIN were at Sheraton hotel, in Oklahoma City. B.R. tried to leave the hotel room because MARTIN was drunk and became "mean." B.R. tried to leave two times, and both times MARTIN grabbed B.R., slammed her onto the bed, and restrained her. MARTIN told B.R. if she does not help get him out of his criminal charges, he will kill himself and it will ruin his family.

22. On May 5, 2024, B.R. and MARTIN were at her house in Broken Arrow. MARTIN knew about B.R.'s meeting with federal agents scheduled for May 6, 2024, and told her to lie about what happened and told her what to say. MARTIN had B.R. rehearse her statements repeatedly to practice.

23. On May 6, 2024, I met with B.R., her attorney Pamela Rains, and AUSA Stacey Todd at the U.S. Attorney's Office. B.R. attempted to recant the rape allegations and said that even though she "knew how the recording sounded," it was a consensual encounter.

24. On May 9, 2024, B.R. sent MARTIN an email and asked him not to contact her and told him she was going to file a protective order. B.R. went to the Tulsa County Courthouse to file a protective order against MARTIN. The Tulsa County Courthouse is located at 500 S. Denver Avenue, Tulsa, Oklahoma, which is located within the Muscogee (Creek) Nation Reservation in the Northern District of Oklahoma. As B.R. was leaving the courthouse, MARTIN walked up behind her and was crying and yelling at her and told her she was going to ruin his life. MARTIN followed B.R. back to her car and got into her car. B.R. told him to get out

of the vehicle and eventually he got out. As she tried to leave, MARTIN blocked the car and prevented her from leaving. B.R. rolled down her window and told him to move out of the way. MARTIN then tried to climb into her car through the window. B.R. began screaming and MARTIN left the area.

25. On May 9, 2024, at approximately 5 pm, an arrest warrant was issued for MARTIN in case 24-MJ-337-MTS. Tulsa Police and the FBI searched for MARTIN all evening, and he was able to evade arrest. At approximately 7:34 am on May 10, 2024, MARTIN texted a TPD officer and said he would surrender. MARTIN then called B.R. and said he just wanted to see her one last time. The FBI became very concerned that MARTIN might attempt violent action based on his previously suicidal statements and erratic behavior. TPD obtained an exigent ping on MARTIN's phone. TPD was able to locate him walking toward his truck outside of his apartment. TPD officers gave MARTIN commands to stop, and MARTIN reached into his truck, giving officers severe safety concerns and concerns that he may have a firearm. After being ordered to stop again, MARTIN became compliant and was taken into custody. MARTIN asked the officers to leave his truck unlocked.

26. MARTIN had his briefcase on his person when he was arrested. Inside his briefcase, we located handwritten notes, with statements about what to tell B.R. to say to the FBI, what demeanor she should adopt during her meeting with the FBI, what questions the FBI was likely to ask, and that she should say the sex was consensual.

27. MARTIN's ex-girlfriend L.M. was also interviewed. L.M. and MARTIN dated from 2020 to 2021. L.M. said that MARTIN raped her on at least one occasion. L.M. said that despite blocking MARTIN and telling him not to contact her, he continued to contact her via phone. He sent her repeated text messages and voice messages. He also showed up to her home uninvited on multiple occasions. L.M. currently has an active domestic violence protective order against MARTIN, in Tulsa County case PO-2021-3387. MARTIN was present at and participated in a hearing on October 27, 2021, where the Court granted a final protective order for 5 years, and by its terms explicitly prohibited the use, attempted use, or threatened use of physical force against his former intimate partner and her child. L.M. has reported several violations of the protective order, after MARTIN contacted her via the phone.

28. Another ex-girlfriend of MARTIN's, V.J., reported that MARTIN raped her several times. They initially met in 2021 via a dating app. Their relationship ended in approximately October of 2021. Once their relationship ended, Martin sent V.J. repeated text messages, voicemails, and called her. When she blocked his phone number, he called from the *67 feature in order to connect the phone call. He also utilized other phone numbers. V.J. was unsure what apps or other methods he utilized to accomplish this. He also contacted her via social media. V.J. was so fearful of Martin she moved and changed her phone number so that he could not find her.

29. At all times relevant, B.R. was a member of the Cherokee Nation by blood and enrollment, roll number 260171. MARTIN is not Indian, as confirmed by B.R. and the five major tribes of Oklahoma, Cherokee, Muscogee (Creek) Nation, Choctaw, Seminole and Chickasaw.

30. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession in the following way: the phone was seized incident to MARTIN's arrest, on May 10, 2024.

31. The Device is currently in storage at the FBI Tulsa Resident Agency, located at 8023 E 63rd Pl, Tulsa, OK. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

Technical Terms

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone.

In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media

player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for

example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

33. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including cyberstalking, witness tampering and domestic violence. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

36. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between

individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like “Snapchat” and “GroupMe.” Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include cyberstalking, witness tampering, and sexual assault.

37. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and

when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

19. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information

subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

20. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

21. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Audra Rees', is written over a horizontal line.

Audra Rees
Special Agent
FBI

Subscribed and sworn to by phone on May 17, 2024.

A handwritten signature in black ink, reading "Christine D. Little". The signature is written in a cursive style with a horizontal line underneath it.

CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

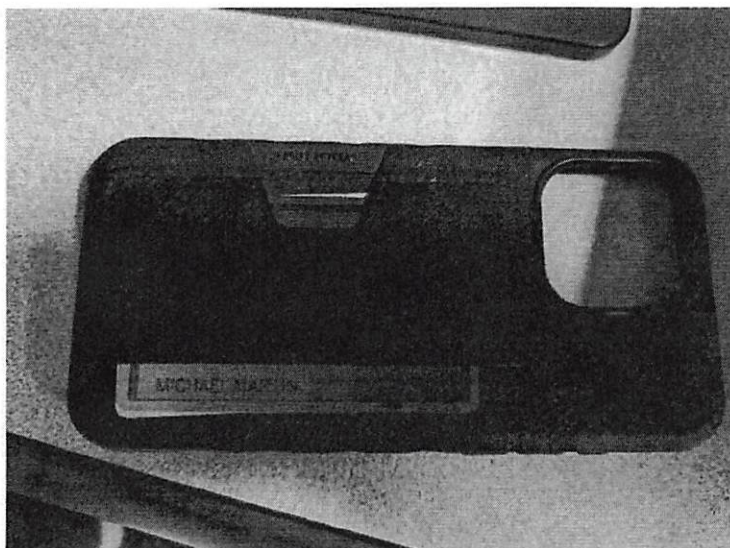
Property to be Searched

The property to be searched is an Apple iPhone 15, Model A2849, with a black case containing a credit card holder, hereinafter the "Device." The Device is currently located at the FBI Tulsa Resident Agency, located at 8023 E 63rd Pl, Tulsa, OK.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

The cell phone to be searched is described above and pictured below:





ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of Title 18, United States Code, Sections 1151, 1153, and 2242(3) (Sexual Abuse without Consent in Indian Country), Title 18, United States Code, Section 2261A (Cyberstalking), and Title 18, United States Code, Section 1512 (Witness Tampering), including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and

cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. Threatening communications related to the criminal offense(s) listed above;
6. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
7. All records and information related to the geolocation of the Device(s) and travel in furtherance of the criminal offense(s) listed above; and
8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate

evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.